コースコード：EC-CSA
税込価格：300,300円 (税抜価格：273,000円)
日数：3日間

---

## 前提条件

・ネットワークの概念 ・TCP/IPプロトコルスイート、セキュリティ技術（Firewall、IDS/IPSなど）、サイバー脅威などに関する基本的な理解を有していること。

## 受講対象者

・SOC（L1およびL2）業務を担当されている方
・SOCアナリストを目指す方、
・ネットワークセキュリティエンジニア
・セキュリティ運用者

## コース概要

このコースは、SOCアナリストとしての高い技術スキルを習得するのに役立つトレーニングと国際認定資格取得をするためのプログラムです。
SOCチームで活躍できるSOCレベル2のスキルを習得すことが可能です。
集中的な 3 日間の講習で SOC 運用全体の基本を理解し、「ログの管理と関連付け」「SIEM の展開」「高度なインシデント検出」「インシデント対応」のような対応を可能とします。

・このコースは、受講後30日間視聴可能なプレイバック動画のZoom URLを提供いたします。
・テキストは、オフラインでも閲覧可能な電子テキストと、印刷テキスト提供します。
・コース初日の7営業前後に BSI.PSJ社より、印刷テキスト送付先住所の確認メールが届きます。
・本コースで使用する追加資料は、ASPEN (EC-Councilのポータルサイト) の「SOC-Tools」から入手可能です (英語資料) 。
・受講料の中に受験料 (1回分) が含まれています。受験は後日、各自で申込みとなります。

## 目的

・SOC運用の基礎を理解し、「ログの管理と関連付け」、「SIEMの理解・運用」、「インシデント検出と対応」を習得する。
・SOCプロセスを理解し、必要な時に上位のアナリストおよびCSIRTと協力した対応ができるスキルを習得する、
・国際認定資格CSA試験に合格する

## アウトライン

1. セキュリティの運用と管理
2. サイバー脅威、IoC、攻撃手法の理解
3. インシデント、イベント、ロギング
4. SIEM（セキュリティ情報およびイベント管理）によるインシデント検知
5. スレットインテリジェンスによるインシデント検知の強化
6. インシデントレスポンス